Fall 2014
SEI Research Review
Contract-Based Integration of CPS Analyses

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Dionisio de Niz
Team: Sagar Chaki (SEI), Ivan Ruchkin (ISR), David Garlan (SCS)

October 28th, 2014

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
28 OCT 2014	**N/A**	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Contract-Based Integration of CPS Analyses - SEI Research Review	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
; ; Chaki /Dionisio de Niz SagarRuchkin /IvanGarlan /David	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**13**	

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM-0001790

Motivation

The development of Cyber-Physical Systems (aircrafts, cars, trains, robots, etc.) increasingly relies on many types of analyses from different disciplines for assurance purposes

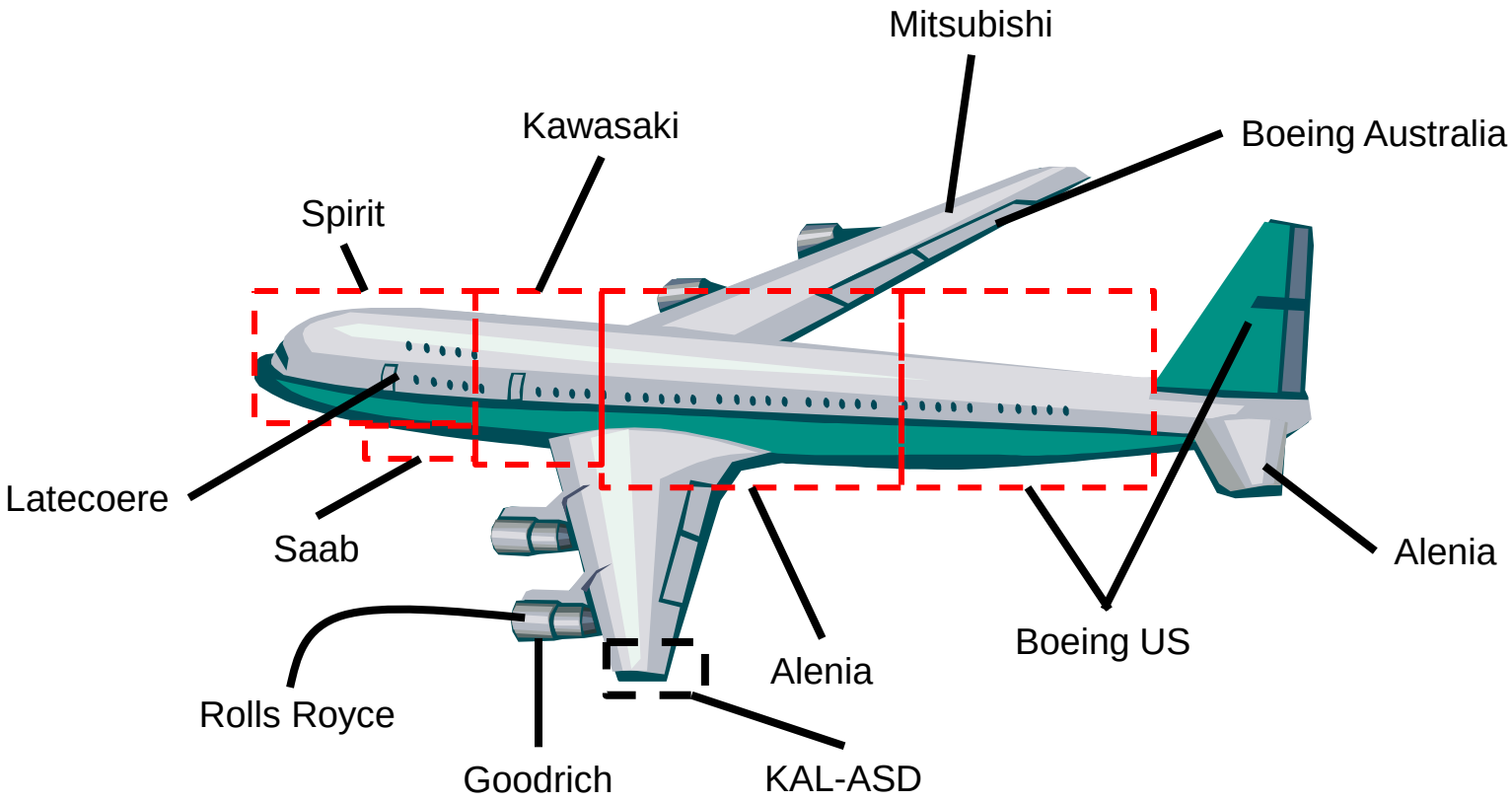
- Control stability, scheduling, logic, thermal, power, aerodynamics, etc.

Large CPS are integrated out of components developed by suppliers that use their own analysis methods and make their own assumptions

Analysis assumption mismatches are discovered late in the system integration phase

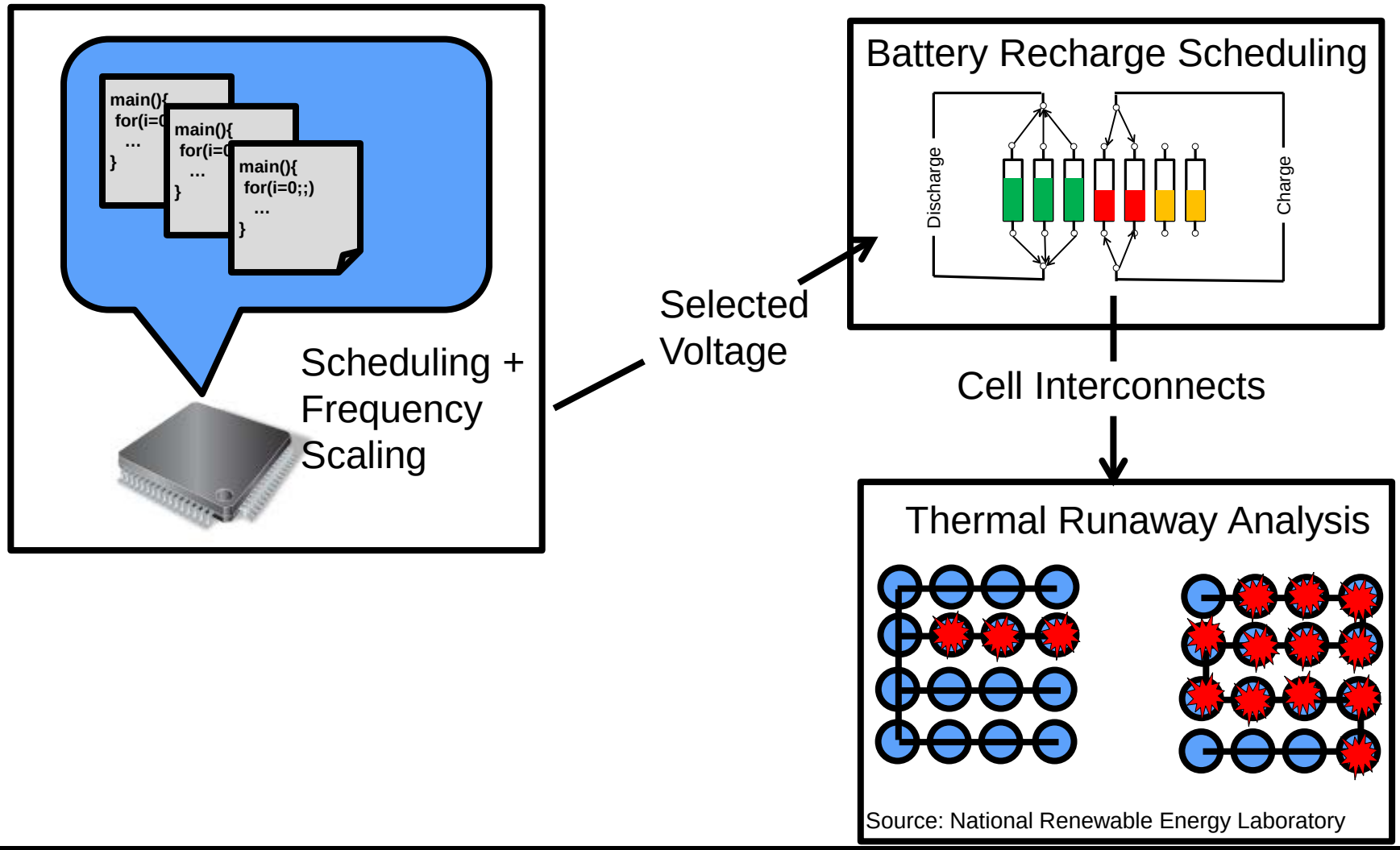
- Difficult and costly to solve

Boeing 787 Suppliers

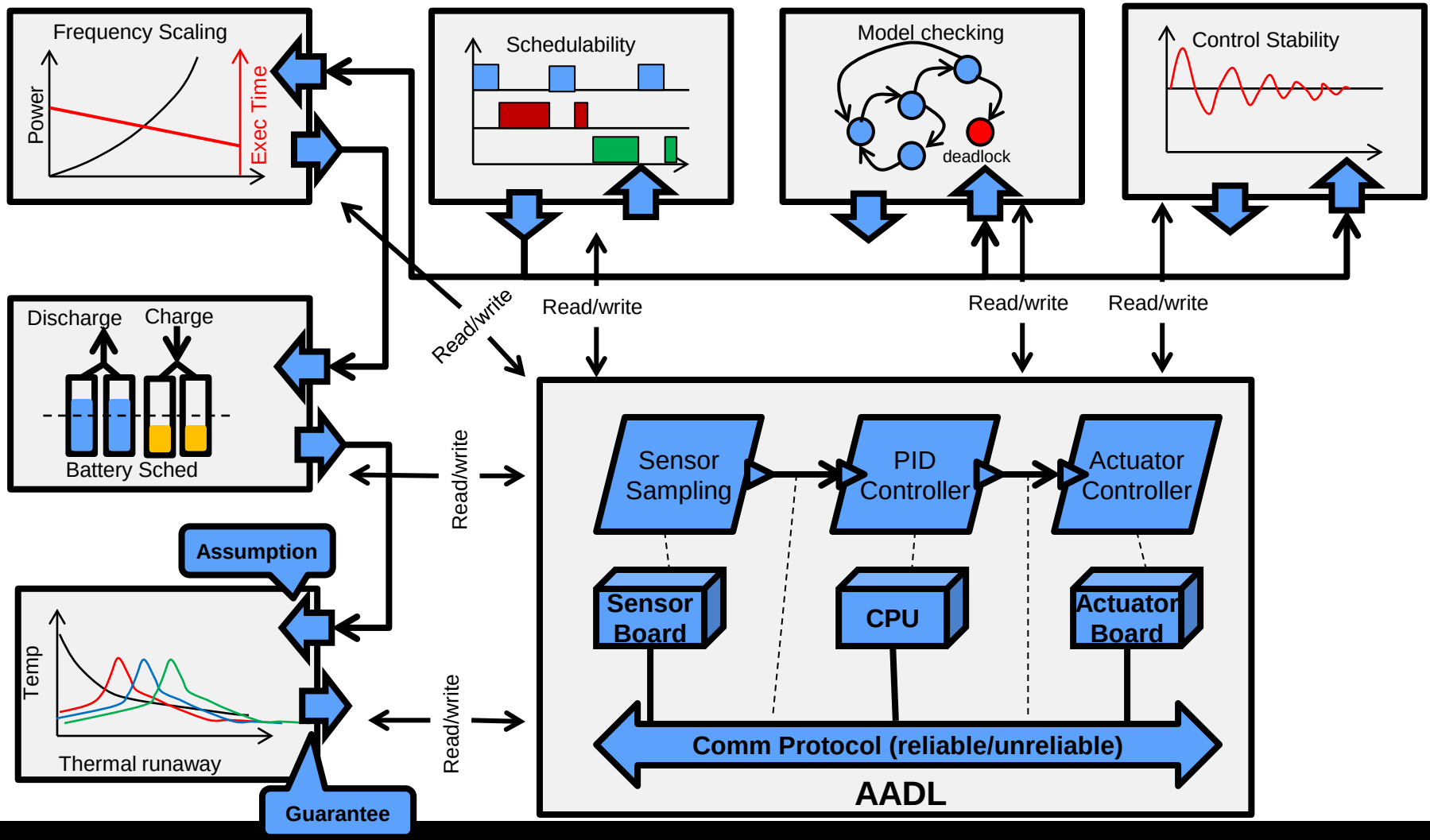


Source: Boeing / Reuters

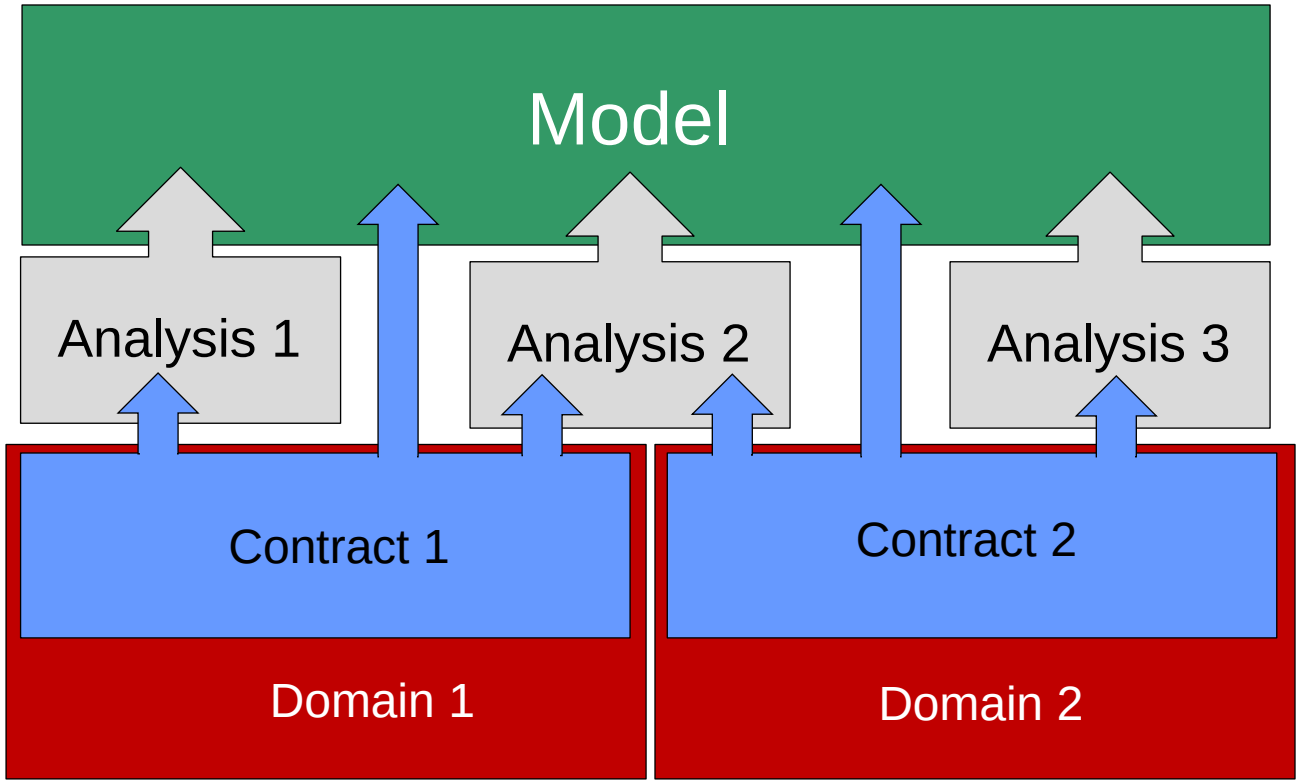
Analyses Interactions



Analysis Contracts



Analysis Contract Scheme



Contract Language & Verification

Contract formulas

- Given domain $\sigma = (\mathcal{A}, \mathcal{S}, \mathcal{R}, \mathcal{T}, [\![\cdot]\!]_\sigma)$,
- $\mathcal{F}_\sigma ::= \forall\, v_1, \ldots, v_j \cdot \phi \mid \exists\, v_1, \ldots, v_j \cdot \phi \mid \forall\, v_1, \ldots, v_j \cdot \phi : \psi \mid \exists v_1, \ldots, v_j \cdot \phi : \psi$
  - $v_i : A_i$, ϕ: static (first order) formula
  - ψ : LTL formula

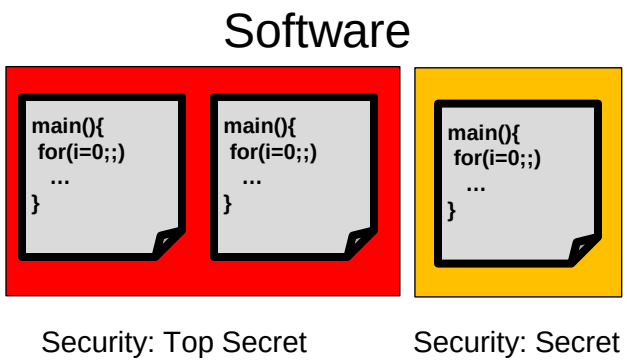
Contract $C = (I, O, A, G)$

- $I \subseteq (\mathcal{A} \cup \mathcal{S})$: Sorts and properties read by the analysis
- $O \subseteq (\mathcal{A} \cup \mathcal{S})$: Sorts and properties written by the analysis
- $A \subseteq \mathcal{F}_\sigma$: assumptions: must be true in input
- $G \subseteq \mathcal{F}_\sigma$: guarantees: must be true in output

Verification

- Contract (& analysis) dependency: $\mathrm{d}(\mathrm{C_i}, \mathrm{C_j}) : \mathrm{C_i}.\mathrm{I} \cap C_j.O \neq \emptyset$
- First order: in SMT (Z3), LTL : Model checker

Example: Surveillance Aircraft



Analysis

Security: tasks of different level to different processor

Scheduling: meet all deadlines

Freq. Scaling: minimize power

Logic: no deadlocks or race conditions

Battery scheduling: meet battery lifetime

Battery thermal: no runaways

Surveillance Aircraft Contracts

Security Analysis

- $An_{sec}.C{:}\, I = \{T, ThSecCl\}, O = \{NotColoc\}, A = \emptyset, G = \{g\}$
  - $g{:}\, \forall\, t_1, t_2 \cdot ThSecCl(t_1) \neq ThSecCl(t_2) \Rightarrow t_1 \in NotColoc(t_2)$

Multiprocessor scheduling: (Binpacking + scheduling)

- $An_{sched}.C{:}\, I = \{T, C, NotColoc, Per, WCET, Dline\}, O = \{CPUBind\}, A = \emptyset, G = \{g\}$
  - $g{:}\, \forall\, t_1, t_2 \cdot t_1 \in NotColoc(t_2) \Rightarrow CPUBind(t_1) \neq CPUBind(t_2)$

Frequency Scaling

- $An_{freqsc}.C{:}\, I = \{T, C, CPUBind, Dline\}, O = \{CPUFreq\}, G = \emptyset, A = \{a\}$
  - $a{:}\, \forall t_1, t_2 \cdot CPUBind(t_1) = CPUBind(t_2){:}\, G(CanPrmpt(t_1, t_2) \Rightarrow Dline(t_1) < Dline(t_2)$

Model checking periodic program (REK):

- $An_{rek}.C{:}\, I = \{T, C, Per, Dline, WCET, CPUBind\}, O = \{ThSafe\}, G = \emptyset, A = \{a_1, a_2\}$
- $a_1{:}\, \forall t \cdot Per(t) = Dline(t),\ a_2{:}\, \forall t_1, t_2 \cdot G(Canprmpt(t_1, t_2) \Rightarrow G\, \neg CanPrmpt(t_2, t_1))$

Thermal runaway:

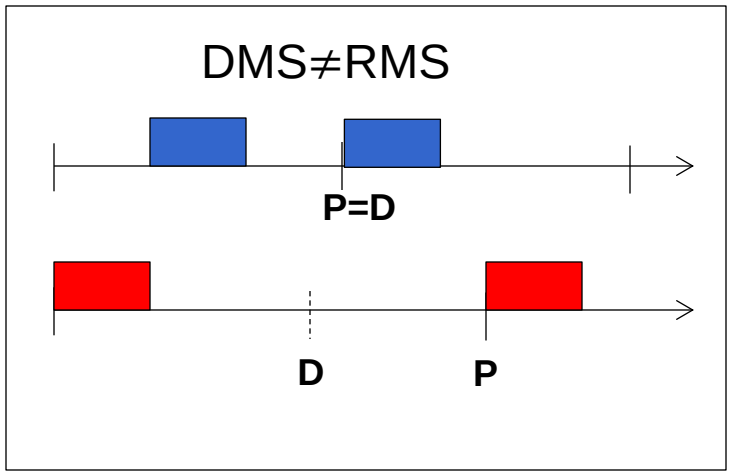
- $An_{therm}.C{:}\, I = \{B, BatRows, BatCols, Voltage\}, O = \{K\}, A = \emptyset, G = \emptyset$

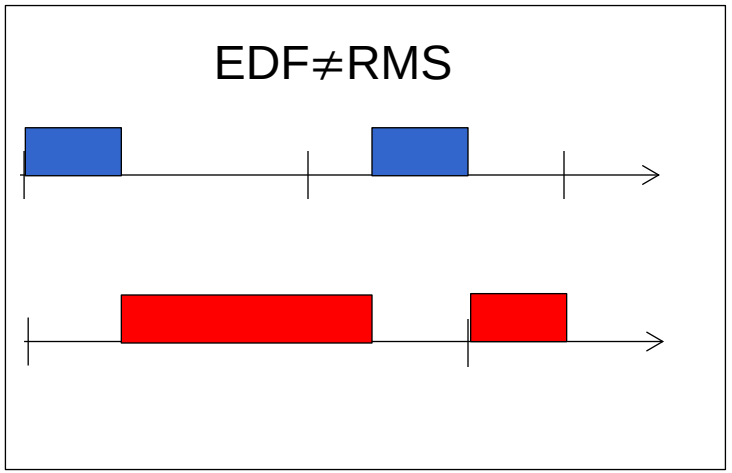
Battery Scheduling

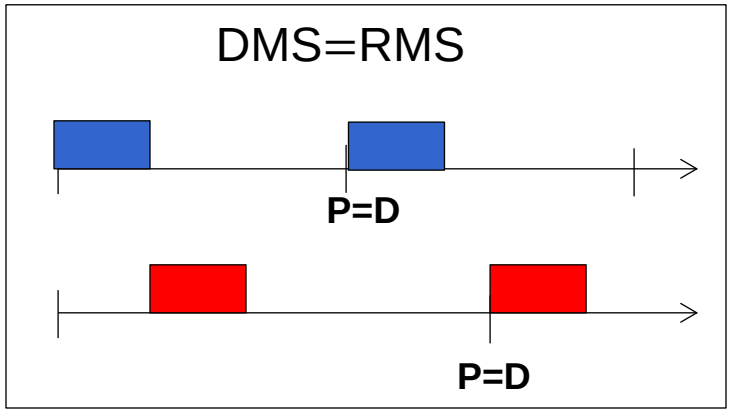
- $An_{bsched}.C{:}\, I = \{B, BatRows, BatCols\}, O = \{BatConnSchedPol, HasReqLifetime, SeriqlReq, ParalRea\}, A = \emptyset, G = \{g\}$
- $g{:}\, G(K(0) \times TN(0) + K(1) \times TN(1) + K(2) \times TN(2) + K(3) \times TN(3) \geq 0)$

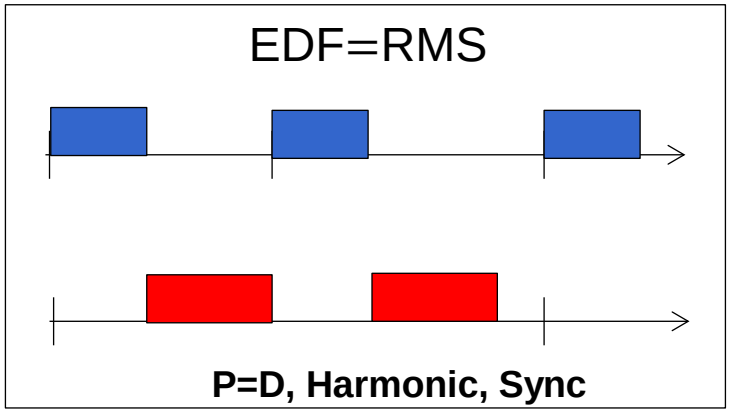
Frequency Scaling Assumption

$a: \forall t_1, t_2 \cdot CPUBind(t_1) = CPUBind(t_2): G(CanPrmpt(t_1, t_2) \Rightarrow Dline(t_1) < Dline(t_2)$









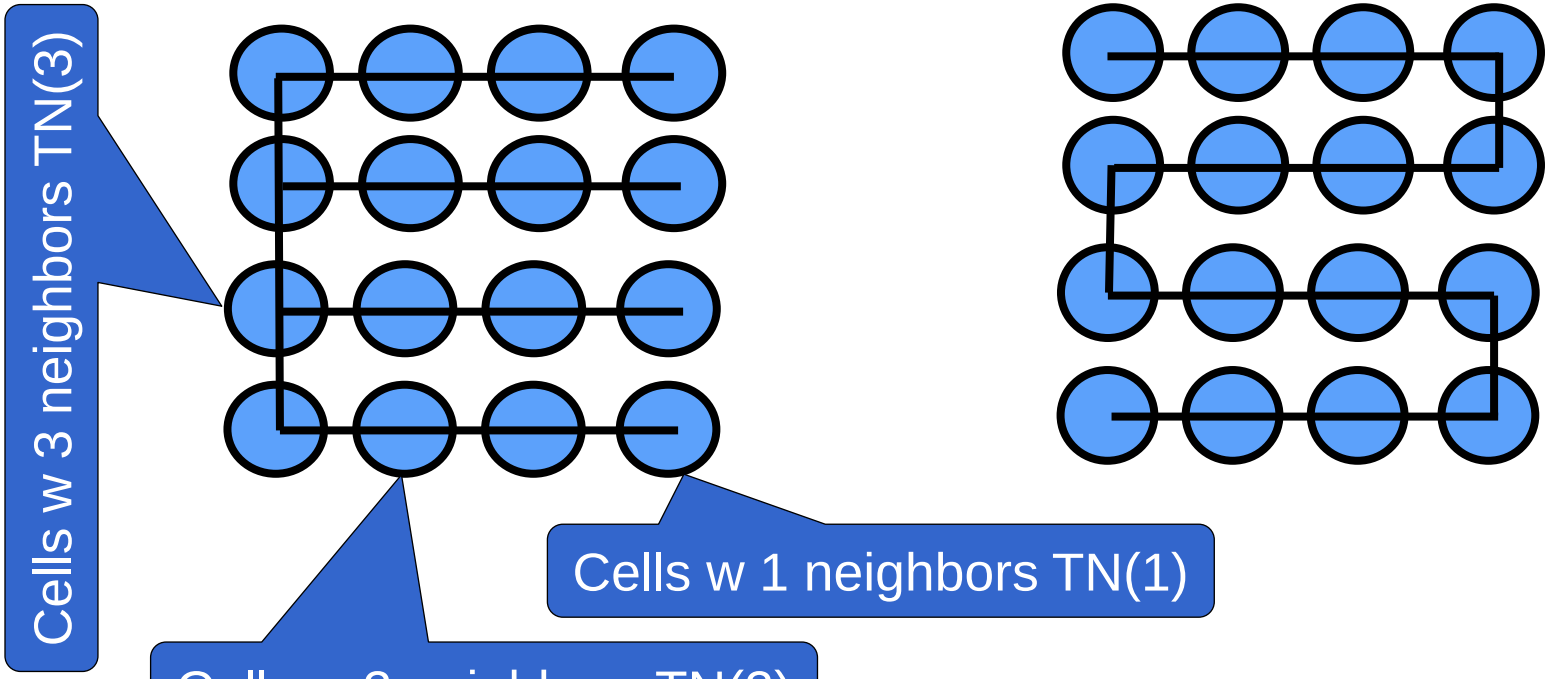
Battery Scheduling Assumption

$$g: G(K(0) \times TN(0) + K(1) \times TN(1) + K(2) \times TN(2) + K(3) \times TN(3) \geq 0)$$

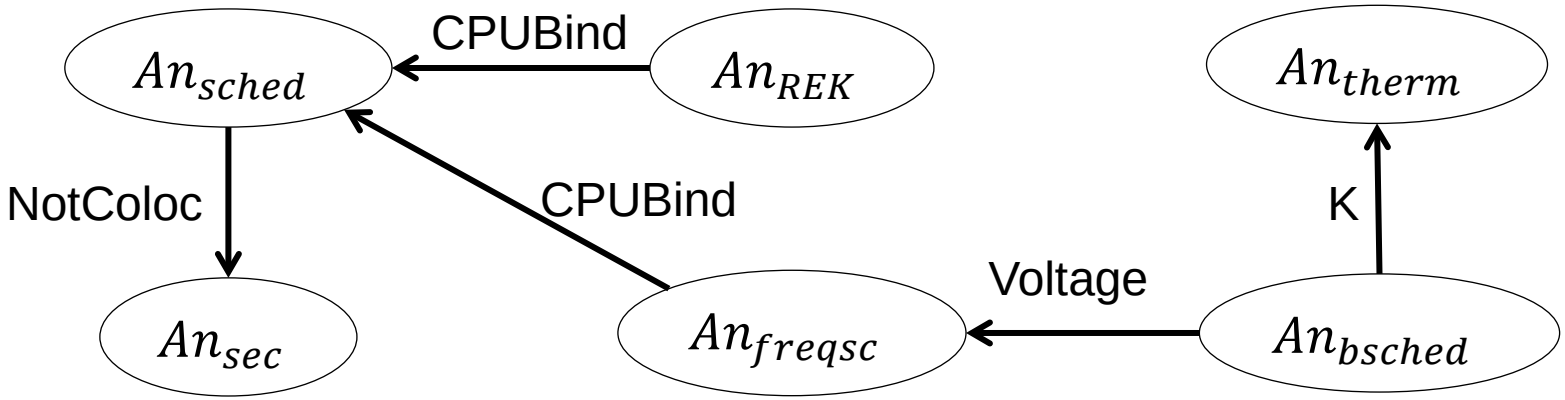
Ratio of cells with 0,1,2,3 neighbors: $1 \cdot TN(1) - 1 \cdot TN(2) + 10 \cdot TN(3) \geq 0$

$$1 \cdot 4 - 1 \cdot 10 + 10 \cdot 2 = 14 \geq 0$$

$$1 \cdot 2 - 1 \cdot 14 + 10 \cdot 0 = -12 < 0$$



Analyses Dependencies



Implementation

Models in the Architecture Analysis and Design Language (AADL)

- Supports multiple analysis
- Supports language extensions (subannexes)
- OSATE Implementation

Analysis Contract Annex

- Implement contract language
- Generates model interpretation

Contract formulas verification

- First Order Logic (Static): SMT / Z3
- LTL (Runtime): Model checking / SPIN

I. Ruchkin, D. de Niz, S. Chaki, and D. Garlan. "Contract-Based Integration of Cyber-Physical Analyses." EMSOFT 2014.

Contact Information

Dionisio de Niz
Senior MTS
CSD/CSC
Telephone: +1 412-268-9002
Email: dionisio@sei.cmu.edu

U.S. Mail
Software Engineering Institute
Customer Relations
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
USA

Web
www.sei.cmu.edu
www.sei.cmu.edu/contact.cfm

Customer Relations
Email: info@sei.cmu.edu
Telephone: +1 412-268-5800
SEI Phone: +1 412-268-5800
SEI Fax: +1 412-268-6257